UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,116	12/02/2003	Victor Gorelik		2789

7590 05/30/2007

Dr. Victor Gorelik
Apt. C1
254 73 Street
Brooklyn, NY 11209

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,116	GORELIK, VICTOR	
	Examiner	Art Unit	
	Oscar A. Louie	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 04/09/2007. Claims 1-5 are pending and have been considered as follows.

Examiner's Notes

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 5 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Buffam (US-6185316-B1).

Claim 1:

Buffam discloses a method for securely submitting biometric data from a client to a server comprising the steps of,

- "performing sampling of a real biometric characteristic at the client" [Fig 8].
- "shuffling arrays of real biometric characteristics in the sequence known at client only to thereby generate twisted biometric data" (i.e. "Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

  It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key.

The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template") [column 12 lines 4-27].

- "submitting the twisted biometric data from the client to the server" [Fig 11 Box# 11].

Claim 2:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 1 above further comprising the steps of,

- "shuffling sequence is calculated at client on the base of the value of a secret object created at the client and known to client only" (i.e. "Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false

image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template") [column 12 lines 4-27].

Claim 3:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 2 above further comprising the steps of,

- "step of multiplying the arrays of biometric characteristics by the sequences of numbers fixed for each type of array and known at the client only" (i.e. "Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false

image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template") [column 12 lines 4-27].

Claim 4:

Buffam discloses a method for securely submitting biometric data from a client to a server as in Claim 3 above further comprising the steps of,

- "step of submitting of twisted biometric data is followed by the step of comparing this data against the samples of twisted biometric data saved at the server previously, in such a way, that the result of the verification and or identification depends neither on the specific sequence in which biometric arrays were shuffled on the client, nor on the specific sequence of numbers used on the client to change the values of the arrays" [Fig 11 Box# 11].

Claim 5:

Buffam discloses a system for secure use of biometric data comprising,

- "the means for performing of twisted sampling and submitting data to the server according to claim 3" (i.e. "Typically, an original image is represented by many discrete information points, similar to grid points on a map. True image points can be extracted from the information points on the basis of pragmatic considerations, such as data

reduction. The set of true image points can be stored as a master template uniquely representative of the original image. False image points are generated and are selectively interposed among a chosen subset of the true image points, forming a transient template. The false image points also may be transformed to produce an encoding key.

It is most preferred that the encoding key itself is the result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. When properly interposed among the chosen true image points, the false image points are essentially indistinguishable from the true image points without reference to the master template, the original image, or complete knowledge of the false image points. These false image points thus form the basis for the secret encryption key. The encoding key can be used to encrypt a portion of plaintext into cipher text, and at least the cipher text portion can be added to the minutia points in the transient template") [column 12 lines 4-27].

- "the means for client verification and or identification according to claim 4" (i.e. "To self-authenticate, the claimant image is used to produce corresponding true image points that are extracted from the true image points of the original image held in the transient template. The residual image points include false image points. Candidate false image points (or minutiae) can be iteratively selected, and hashed to form a decryption key, with the decryption key operating on the cipher text to produce a result which is compared with the original, known plaintext. If the decryption result does not favorably compare,

the steps of candidate image point reselection, decryption key generation, cipher text decryption, and comparison with the known plaintext continues, until the pools of candidate false image points is exhausted, or a policy limitation is reached") [column 13 lines 6-19].

Response to Arguments

4. Applicant's arguments filed 04/09/2007 have been fully considered but they are not persuasive. Applicant's argument regarding Claim 1 is non-persuasive since the shuffling of a sequence is equivalent to hashing, encrypting, encoding, etc. Cryptography procedures such as hashing, encrypting, and encoding commonly are associated with scrambling data or any information from one form to another (i.e. shuffling) to make it difficult to recover unless the individual is a valid user or owner of that information. There are many algorithms with mathematical formulas typically used for the scrambling of information in order to protect it (commonly known as encryption). Arguments regarding Claim 2 are non-persuasive since the combining of hashed false image points and true image points would succeed by means of a similar procedure as "shuffling" of a sequence of values in a biometric array. In regards to the applicant's arguments to Claim 3, the two procedures as disclosed by Buffam and the applicant are equivalent. This is because the false image points (i.e. sequence of values) are hashed resulting in the encoding key (i.e. multiplied by the sequence of numbers known to the user only). The user with the proper associated credentials would only know the encoding key. The applicant's arguments in regard to Claim 4 are non-persuasive because in the context of Buffam,

decoding is equivalent to a comparison of two twisted signatures. If the decoding succeeds, it implies that the decoding keys are the same on both ends of the client and server (i.e. "client side is compared with the twisted signature saved on the server...if the claimant is the correct person, these signatures match). In regards to Claim 5, the invention as disclosed by Buffam is equivalent to the applicant's invention, thus, any system incorporating the method disclosed by Buffam would be encompassed.

In regards to section "B. Claim Rejections: broad scope argument" of the applicant's remarks and arguments, it is noted by the examiner that publicly editable sources of information such as Wikipedia™ are not reliable sources of information, particularly for priority dates and other citation proof purposes. In addition, the specifically use of MD5 is not suggested by Buffam. The disclosure of such was only intended as an example of a hash algorithm that may be used. Therefore, it would be anticipated that one of ordinary skill in the art would be aware of such limitations and weaknesses, and would choose a more secure algorithm/method for their usage. It is also noted that the weakness of MD5 hashing is minimal due to the circumstances of the implementation of MD5. The examiner points to the disclosure by SecurityFocus™,

"Applications that implement the APOP protocol may be vulnerable to a password-hash weakness. This issue occurs because the MD5 hash algorithm fails to properly prevent collisions.

Attackers may exploit this issue in man-in-the-middle attacks to potentially gain access to the first three characters of passwords. This will increase the likelihood of successful brute-force attacks against APOP authentication.

To limit the possibility of successful exploits, applications that implement the APOP protocol should set up safeguards to ensure that message IDs are RFC-compliant." This applies to many other applications of MD5 hashing. From an academic standpoint, the vulnerability is critical, however, from an implementation point of view, the threat is next to none since one of ordinary skill in the art would recognize the precautionary measures that may be taken to mitigate this risk. The threat of social engineering or internal leaks by malicious employees is much greater due to them being inexpensive and less time consuming than heavy computational brute-forcing as is necessary for exploiting the weakness in MD5.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
05/24/2007

James Myhre
Supervisory Patent Examiner